REMARKS

Claims 1-34 remain in this application. No claims have been added, canceled, or amended in this reply.

ALLOWABLE SUBJECT MATTER

The Office Action indicated that Claims 7-11, 18-22 and 29-33 are directed to allowable subject matter.

CLAIM REJECTIONS – 35 U.S.C. § 103

The Office Action rejected Claims 1-6, 12-17, and 23-28, and 34 under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent No. 6,209,104 ("Jalili") in view of U.S. Patent No. 6,535,980 ("Kumar"). The rejection is respectfully traversed.

Independent Claim 1 recites a method for verifying the legitimacy of an untrusted mechanism. The method comprises:

> **submitting a first set of information and a second set of information to an untrusted mechanism in a sequence that is unpredictable to the untrusted mechanism;**
>
> receiving a response from the untrusted mechanism for each submission of either said first set of information or said second set of information;
>
> determining whether each response received from the untrusted mechanism is a correct response; and
>
> in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, **determining the untrusted mechanism to not be legitimate.**

The method of Claim 1 is quite advantageous because it provides an effective means for testing the legitimacy of any untrusted mechanism. According to the method, an untrusted mechanism is determined to not be legitimate if any of the untrusted mechanism's responses to a sequence of information set submissions is an incorrect response. Because the sequence in which information sets are submitted to an untrusted mechanism is unpredictable to the untrusted mechanism, it is highly difficult, if not impossible, for an illegitimate untrusted mechanism to "fake" correct responses to all of the submissions.

Jalili does not teach or suggest such a method. Instead, Jalili discloses a technique whereby information that identifies a password can be transmitted over a network without transmitting the actual password over the network, thereby preventing malicious parties from intercepting and using the password. More specifically, Jalili discloses that a server generates an image that contains randomly arranged icons. Each icon represents a different number or letter. The server stores position correlation information that correlates the position of each icon with the number or letter that the icon represents. The server sends the image—but not the position correlation information—to a client, which displays the image to a user. The user selects icons from the image, in the same way that the user would select numbers and letters from a keyboard or keypad, to input the user's password. However, instead of transmitting the actual password to the server over the network, the client transmits only the positions of the icons that the user selected. The server receives the positions and uses the position correlation information to determine the numbers or letters to which the positions correspond, thereby constructing the actual password at the server. The server then determines whether the password is correct. A malicious party that intercepts the positions transmitted over the network cannot derive the password from the positions because the malicious party does not possess the position correlation information.

Indeed, the Office Action concedes that Jalili fails to disclose "submitting a first set of information and a second set of information to an untrusted mechanism in a sequence that is unpredictable to the untrusted mechanism" as recited in Claim 1. The Office Action only alleges that Jalili discloses "submitting information to an untrusted mechanism."

However, Jalili does not teach or suggest "submitting information **to an untrusted mechanism**," because Jalili's client and Jalili's server **trust each other**; Jalili's technique is designed to prevent parties **other than the server** from using intercepted data to determine a password. There is no teaching or suggestion in Jalili that the client and the server do not trust each other. The authenticity of the user that uses the client may be in question, but **a user is a person rather than a mechanism.**

Jalili's client **submits** data **to** Jalili's server; although it is possible that a malicious party might **intercept** such data, Jalili's client certainly does not **submit** such data **to** such a malicious party! The interception of data by a malicious party does not imply that the data was **submitted to** the malicious party. Therefore, Jalili, taken individually, fails to teach or suggest "submitting information . . . **to an untrusted mechanism**" as recited in Claim 1.

The Office Action relies upon Kumar to disclose, allegedly, that "information" may be a first set and a second set that are in a sequence that is unpredictable to an untrusted mechanism.

Kumar discloses a technique for cryptographically and keylessly protecting a message by coding and transmitting a message as a binary string—all "ones" and "zeroes." Kumar discloses that a correct ("true") response to a receiver's challenge is sent in order to represent a "one" in a binary-coded message, and a deliberately incorrect ("false") response to a receiver's challenge is sent in order to represent a "zero" in the

binary-coded message. Thus, Kumar discloses a technique for sending a message in a secret fashion.

However, Kumar's technique has nothing to do with submitting information **to an untrusted mechanism**. Even if Kumar discloses sending sets of information in sequences, Kumar still fails to teach or suggest that such sequences are **submitted to an untrusted mechanism**. In Kumar, **a sender sends information to a receiver that the sender trusts**. Kumar's sender does not submit information **to** a malicious party that might be trying to intercept the information. Therefore, Kumar, taken individually, fails to teach or suggest "submitting information . . . **to an untrusted mechanism**" as recited in Claim 1.

It is apparent from the discussion above that neither Jalili nor Kumar individually teaches or suggests "submitting information . . . **to an untrusted mechanism**" as recited in Claim 1. This is not surprising, since neither Jalili nor Kumar are concerned with authenticating an untrusted mechanism. Consequently, even if Jalili and Kumar were combined (assuming, *arguendo*, that one would have been motivated to combine these references), the combination still would not disclose, teach, or suggest "**submitting** a first set of information and a second set of information **to an untrusted mechanism** in a sequence that is unpredictable to the untrusted mechanism" as recited in Claim 1. Therefore, Claim 1 is patentable over Jalili and Kumar, taken individually or in combination, under 35 U.S.C. § 103(a).

Additionally, neither Jalili nor Kumar ever determines an untrusted mechanism to be illegitimate. As is discussed above, neither Kumar nor Jalili are concerned with the legitimacy of any mechanism. The Office Action alleges that Jalili discloses such a determination at col. 8, lines 14 and 15, which merely say: "If so, the user will be allowed appropriate access to the server subsystem." The user may be denied access to the server if he enters the wrong password, but it does not follow from this that the legitimacy of the

client that the user used to enter the wrong password is ever in question. Although the authenticity of the user may be in question, **a user is a person rather than a mechanism**.

Furthermore, one of ordinary skill in the art at the time of the present invention would not have been motivated to combine Jalili and Kumar for the reasons set forth in the Office Action. The Office Action reasons that one would have been motivated to combine Jalili and Kumar because "the challenge response is a suitable method for sending arbitrary messages in a secret fashion."

The Office Action cites Kumar, col. 2, lines 63-67 in support of this proposition. This passage of Kumar indicates that Kumar's technique extends the challenge-response system to change the challenge-response system from a mere authentication system into a secret message-sending system.

Thus, Kumar's technique is useful to send messages secretly (in an encoded form) so that malicious third parties who intercept the messages cannot use those messages to do mischief. A system that lacks the ability to send messages secretly might have some use for Kumar's technique. However, Jalili's system **is not such a system**.

Jalili already has a technique for sending messages secretly; as described above, Jalili sends the positions of user-selected icons to a server instead of an actual password. Malicious parties who intercept the positions cannot use the positions to derive the password because they lack the server's position correlation information, which is not transmitted. Because Jalili's technique already provides a way for sending messages secretly, there is no need to modify Jalili's technique to send messages secretly using Kumar's challenge-response approach. The Office Action provides no explanation as to why Kumar's secret message-sending approach would be any better than Jalili's current secret message-sending approach.

Indeed, it is likely that Jalili's current secret message-sending approach works better in Jalili's overall scheme than Kumar's challenge-response based approach would. In fact, it is unclear how the two systems could be combined in a way that would still work; while alleging that the systems could be combined, the Office Action has not explained **how** the systems could be combined.

Jalili's technique does not need Kumar's challenge-response approach. Jalili's technique cannot even make use of Kumar's challenge-response approach. One of ordinary skill in the art would **not** have been motivated to combine Jalili and Kumar for the reason set forth in the Office Action. The alleged motivation to combine set forth in the Office Action is no motivation at all.

Applicants further submit that Claims 2-6, which depend from Claim 1 and which recite further advantageous aspects of the invention, are also patentable over Jalili and Kumar for at least the reasons given above in connection with Claim 1.

Claims 12-17 are apparatus claims, which are analogous to the methods of Claims 1-6, respectively. Applicants submit that Claims 12-17 are patentable over Jalili and Kumar for at least the reasons given above in connection with Claims 1-6, respectively.

Claims 23-28 are computer-readable medium claims, which are analogous to the methods of Claims 1-6, respectively. Applicants submit that Claims 23-28 are patentable over Jalili and Kumar for at least the reasons given above in connection with Claims 1-6, respectively.

Claim 34 recites, *inter alia*, "submitting a sequence of submissions to an untrusted mechanism." As is discussed above, Jalili and Kumar, taken individually or in combination, do not disclose, teach, or suggest submitting information **to** an untrusted mechanism. It follows that Jalili and Kumar, taken individually or in combination, also do not disclose, teach, or suggest the feature of Claim 34 quoted above. Therefore, Claim 34 is patentable over Jalili and Kumar under 35 U.S.C. § 103(a).

CONCLUSION

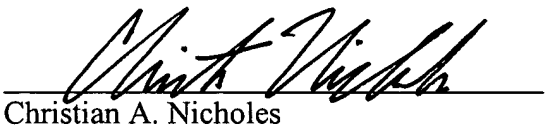
For at least the reasons set forth above, Applicants respectfully submit that all pending claims are patentable over the art of record, including the art cited but not applied. Accordingly, allowance of all pending claims is respectfully solicited.

The Examiner is invited to telephone the undersigned at (408) 414-1080 to discuss any issue that may advance prosecution.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: MARCH 31, 2005



Christian A. Nicholes
Reg. No. 50,266

1600 Willow Street
San Jose, California 95125-5106
Telephone No.: (408) 414-1080
Facsimile No.: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on 3/31/05 by